The Russian invasion of Ukraine has highlighted the long-term energy dependencies on Moscow that Europe will neither be able to resolve quickly, nor without great sacrifice. Russia’s hybrid warfare—a combination of kinetic strikes against key infrastructure, information manipulation, malign finance, economic coercion, and cyber operations—has used Ukraine to target the heart of Europe’s energy security. This war has forced the continent to consider how to realize its economic, environmental, and geostrategic energy goals on its own.

This study found that systemic dependencies and cyber vulnerabilities in critical energy infrastructure throughout the European Continent could impact the Alliance’s political stability and threaten military effectiveness. Forward mobility and troop readiness is affected directly by energy shortfalls and increasing cyber vulnerabilities across NATO. The following main findings related to cyber and malign influence provide a sobering view of the challenges of hybrid warfare on energy security in NATO nations.

**Increased Cyber Threats Threaten Critical Energy Infrastructure**

Russia and its agents have successfully penetrated energy networks in Europe and North America and deployed malware to undermine critical systems and infrastructure in the target country. Since the invasion of the Ukraine, significant cyberattacks have impacted NATO member states.

Advanced critical energy infrastructure warning and cyber threat mitigation systems currently in place are not adequate to ensure safety and resilience when emerging technologies being integrated into energy systems are not cyber secured. There are large differences between NATO member states in cyber mitigation capabilities and standards.

This book identifies potential solutions to mitigate cyberattacks and increase energy independence for militaries of NATO member states and to prevent cyber vulnerabilities to critical energy infrastructure. These options include a new generation of cyber early warning systems and microgridding.
Energy Sector Supply Chain Vulnerabilities Impact Military Operations

Moody’s Analytics has reported that the greatest risk to the global supply chain is now caused by the Russia-Ukraine military conflict, not the pandemic. With Russia supplying 43 percent of Europe’s natural gas and 40 percent of the world’s palladium (used for semiconductors) and Ukraine supplying 70 percent of the world’s neon (used to create computer chips), the prolonged uncertainty of the conflict could continue to affect the global supply chain severely.

Going forward, supply chain components will continue to be subject to major threats from different sub-chains that interact directly with low-security scrutiny. Cybersecurity vulnerabilities in the gas, power, and nuclear industries are pervasive, increasing the threats due to the interactions within each sub-chain.

Strategies for higher supply chain resilience could include: (1) supply chain mapping and modeling to better predict supply and demand, (2) diversifying suppliers, (3) shortening supply chains, and (4) automation with a careful evaluation of cyber risks.

Malign Influence Is Directly Impacting Critical Energy Infrastructure

Russia views cyberattacks, hacking, and the spread of disinformation as instruments of foreign policy and national security interests. Through compromised websites such as news sources and official government sites, Russian operatives published fabricated articles, stories, quotes, and other documents criticizing the United States and NATO’s presence in Eastern Europe. Information operations and malign influence specifically target the energy sector in countries like Poland, Romania, and Germany, with operational and economic impact.

Early detection of disinformation campaigns is crucial to prevent malicious actors from escalating and exploiting this activity. To solve this problem, a task force could be established within NATO’s Joint Intelligence and Security Division to establish a network for detecting and countering disinformation in their nascent stages. The information would then be classified according to its impact, including threat level in terms of timeline, and its possibility of spreading to a local, state, national, or international level.

While these findings and recommendations are not exhaustive, using emerging tools to foster energy independence and cybersecurity while countering malign influence will help NATO navigate from a position of strength and resilience in the conflict-laden days ahead.